UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/655,230	09/05/2000	Chung Nan Chang	2170	7762

7590 08/25/2004

Donald E Schreiber
Donald E. Schreiber A Professional Corp.
Post Office Box 2926
Kings Beach, CA 96143-2926

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/655,230	CHANG, CHUNG NAN	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/7/02,1/22/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-41 have been examined.

Specification

2. Applicant is reminded of the proper content of an abstract of the disclosure.

A patent abstract is a concise statement of the technical disclosure of the patent and should include that which is new in the art to which the invention pertains. If the patent is of a basic nature, the entire technical disclosure may be new in the art, and the abstract should be directed to the entire disclosure. If the patent is in the nature of an improvement in an old apparatus, process, product, or composition, the abstract should include the technical disclosure of the improvement. In certain patents, particularly those for compounds and compositions, wherein the process for making and/or the use thereof are not obvious, the abstract should set forth a process for making and/or use thereof. If the new technical disclosure involves modifications or alternatives, the abstract should mention by way of example the preferred modification or alternative.

The abstract should not refer to purported merits or speculative applications of the invention and should not compare the invention with the prior art.

Where applicable, the abstract should include the following:
(1) if a machine or apparatus, its organization and operation;
(2) if an article, its method of making;
(3) if a chemical compound, its identity and use;
(4) if a mixture, its ingredients;
(5) if a process, the steps.

Extensive mechanical and design details of apparatus should not be given.

3. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The

abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

4. The abstract of the disclosure is objected to because of undue length. Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 40 and 41 are rejected under 35 U.S.C. 102(b) as being anticipated by Crandall U.S. Patent No. 5,581,616 (hereinafter Crandall 5,581,616).

7. As per claim 40, Crandall 5,581,616 discloses within protocol for communication in which a sending unit S transmits onto the communication channel I a message "M" together with a digital signature, and, wherein before transmitting the message M and the digital signature, the sending unit S transmits for storage in a publicly accessible repository a plurality of public quantities (see Crandall 5,581,616, Figures 8-12, especially Figure 12; col. 1, lines 50-56), a method by which a receiving unit R that

receives the message m and the digital signature verifies the authenticity of digital signature comprising the steps performed by the receiving unit R of:

a. retrieving the plurality of public quantities from the publicly accessible repository (see Crandall 5,581,616, col. 1, lines 50-56);

b. using the digital signature and the plurality of public quantities, evaluating expressions of at least two different verification relationships and comparing pairs of results obtained by evaluating the expressions of the at least two different verification relationships (see Crandall 5,581,616, Abstract; Figure 11; col. 20, lines 43-60).

The aforementioned covers claim 40.

8. As per claim 41, Crandall 5,581,616 discloses a method as outlined above in the claim 40 rejection under 35 U.S.C. 103(a). In addition, the plurality of public quantities includes a plurality of vectors by definition of points in n-dimensional coordinate systems used in elliptic curve cryptosystems. See Crandall 5,581,616, col. 6, lines 5-7. The aforementioned covers claim 41.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-5, 12-18, 25-31, 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman et al. U.S. Patent No. 4,200,770 (hereinafter Hellman) in view of Schneier Applied Cryptography (hereinafter Schneier).

11. As per claim 27, Hellman discloses a cryptographic unit adapted for inclusion in a system for communicating as an encrypted ciphertext message M a plaintext message P that has been encoded using a cryptographic key K (see Hellman, Abstract), the system including:

a. a communication channel I adapted for transmitting the ciphertext message M (see Hellman, Figure 1, Reference No. 19 and variable C); and

b. a pair of transceivers that are coupled to the communication channel I, and that are adapted for communicating the ciphertext message M from one transceiver to the other transceiver via the communication channel I (see Hellman, Figure 1, Reference Nos. 31 and 32);

the cryptographic unit being adapted for coupling to the transceivers for transmitting the ciphertext message M thereto or receiving the ciphertext message M therefrom (see Hellman, Figure 1, Reference Nos. 11 and 12), and comprising:

c. ports (see Hellman, Figure 1, coupling between Reference Nos. 15, 16, 21, 22, 25, 26, 31 and 32):

i. when the cryptographic unit is to receive the ciphertext message M, for:

(1) receiving via the communication channel I a plurality of sender's quantities from a sending cryptographic unit (see Hellman, Figure 1, variables: q, a, Y1 and related text), and the receiving cryptographic unit using the plurality of sender's quantities and at least some of a plurality of public quantities in computing:

(a) at least one receiver's quantity which the receiving cryptographic unit transmits via the communication channel I to the sending cryptographic unit (see Hellman, Figure 1, variable Y2 and related text); and

(b) the key K (see Hellman, Figure 1, variable K within Reference No. 12 and related text); and

ii. when the cryptographic unit is to send the ciphertext message M, for generating the plurality of public quantities (see Hellman, Figure 1, Reference Nos. 21 and 25, and related text), the sending cryptographic unit using the generated plurality of public quantities in computing:

(1) the plurality of sender's quantities which the sending cryptographic unit transmits via the communication channel I to the receiving cryptographic unit (see Hellman, Figure 1, variables q, a, Y1 and related text); and

(2) after receiving via the communication channel I the receiver's quantity from the receiving cryptographic unit, the key K

(see Hellman, Figure 1, variable K within Reference No. 11 and related text); and

d. a cryptographic device having:

i. a key input port for receiving the key K from the cryptographic unit (see Hellman, Figure 1, port receiving variable K on device represented as Reference No. 15);

ii. a plaintext port:

(1) for accepting the plaintext message P for encryption into the ciphertext message M that is transmitted from the cryptographic device (see Hellman, Figure 1, port receiving variable P on device represented as Reference No. 15), and

(2) for delivering the plaintext message P obtained by decrypting the ciphertext message M received by the cryptographic device (see Hellman, Figure 1, port delivering variable P on device represented as Reference No. 16); and

iii. a ciphertext port that is coupled to one of the transceivers:

(1) for transmitting the ciphertext message M to such transceiver (see Hellman, Figure 1, port coupling device represented by Reference Nos. 21, 22, 31 and 32), and

(2) for receiving the ciphertext message M from such transceiver (see Hellman, Figure 1, port coupling device representing by Reference Nos. 32 and 22).

12. Hellman does not expressly disclose storing a plurality of public quantities in a publicly accessible repository. However, the variables q and a used in Diffie-Hellman key exchange are public variables within a public-key cryptosystem, which enables these public variables to be published in a public repository as taught by Schneier. See Schneier, page 32, 2nd paragraph; page 515, 'Key Exchange Without Exchanging Keys'. Furthermore, a third party repository acts as a disinterested member of a communications system and can ensure the certification, renewal and cancellation of public information. See Schneier, page 23, 'Arbitrated Protocols'. It would be obvious to one of ordinary skill in the art at the time the invention was made to store the plurality of public quantities in a public accessible repository and retrieve the plurality of public quantities from the public accessible repository for secure key exchange to simplify the key exchange process. See Schneier, page 32, 3rd paragraph. The aforementioned covers claim 27.

13. As per claim 28, Hellman covers a cryptographic unit as outlined above in the claim 27 rejection under 35 U.S.C. 103(a). In addition, Schneier teaches the cryptographic unit wherein, when receiving the ciphertext message M, in storing the plurality of public quantities into the publicly accessible repository;

a. selects a receiver's secret quantity (see Schneier, page 513, Step 2, 'y');

b. selects for storage in the publicly accessible repository as part of the plurality of public quantities a plurality of selected public quantities (see Schneier,

page 513, 2nd paragraph; page 515, 'Key Exchange Without Exchanging Keys'); and

c. using the receiver's secret quantity and the plurality of selected public quantities, computes for storage in the publicly accessible repository as part of the plurality of public quantities a plurality of computed public quantities (see Schneier, page 513, Step 2, 'Y').

14. It would be obvious to one of ordinary skill in the art at the time the invention was made to store a plurality of computed public quantities that are computed using the receiver's secret quantity to enable the Diffie-Hellman key exchange steps as taught by Schneier. Ibid. The aforementioned covers claim 28.

15. As per claims 29-31, Hellman covers a cryptographic unit as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). In addition, the plurality of public quantities, the plurality of selected public quantities and the plurality of computed public quantities include a plurality of vectors. See Hellman, col. 8, lines 38-41. The aforementioned cover claims 29-31.

16. As per claim 38, Hellman covers a cryptographic unit as outlined above in the claim 27 rejection under 35 U.S.C. 103(a). In addition, the cryptographic unit wherein, when receiving the ciphertext message M, in computing for transmission to the sending cryptographic unit the at least one receiver's quantity, uses a receiver's secret quantity, at least some of the plurality of public quantities, and at least one of the plurality of

sender's quantities received from the sending cryptographic unit. See Hellman, col. 4, line 67. The aforementioned covers claim 38.

17. As per claim 39, Hellman covers a cryptographic unit as outlined above in the claim 38 rejection under 35 U.S.C. 103(a). In addition, the receiver's quantity includes at least one vector. See Hellman, col. 8, lines 38-41. The aforementioned covers claim 39.

18. As per claims 1-5, 12 and 13, they are method claims corresponding to claims 27-31, 38 and 39, and they do not teach or define above the information claimed in claims 27-31, 38 and 39. Therefore, claims 1-5, 12 and 13 are rejected as being unpatentable over Hellman in view of Schneier for the same reasons set forth in the rejections of claims 27-31, 38 and 39.

19. As per claims 14-18, 25 and 26, they are system claims corresponding to claims 27-31, 38 and 39, and they do not teach or define above the information claimed in claims 27-31, 38 and 39. Therefore, claims 14-18, 25 and 26 are rejected as being unpatentable over Hellman in view of Schneier for the same reasons set forth in the rejections of claims 27-31, 38 and 39.

20. Claims 6-11, 19-24 and 32-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman in view of Schneier, and further in view of Crandall U.S. Patent No. 5,159,632 (hereinafter Crandall 5,159,632).

21. As per claim 32, Hellman covers a cryptographic unit as outlined above in the claim 28 rejection under 35 U.S.C. 103(a). Hellman does not expressly teach the sending unit selecting a one-time parameter, transmitting it to the receiving unit and using the one-time parameter along with the sender's secret quantity and at least some of the retrieved plurality of public quantities to compute the plurality of sender's quantities. However, in a separate section, Schneier discloses techniques using elliptic curves in the Diffie-Hellman key exchange algorithm. See Schneier, page 480, 6th and 8th paragraphs. As known in the art, elliptic curve systems share coordinate points between the receiver and the sender: this one-time parameter is used to define an elliptic curve group used by the relevant public key cryptosystem. Crandall 5,159,632 teaches such a shared one-time parameter used in an elliptic curve cryptosystem. See Crandall 5,159,632, col. 7, lines 57-60. It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Crandall 5,159,632 to the apparatus of Hellman. Motivation for such a combination enables faster public-key cryptosystems with smaller key sizes as taught by Schneier. Ibid. The aforementioned covers claim 32.

22. As per claim 33, Hellman covers a cryptographic unit as outlined above in the claim 32 rejection under 35 U.S.C. 103(a). In addition, the plurality of sender's quantities includes a plurality of vectors. See Hellman, col. 8, lines 38-41. The aforementioned covers claim 33.

23. As per claims 34-37, they are apparatus claims corresponding to claims 32, 33, 38 and 39, and they do not teach or define above the information claimed in claims 32, 33, 38 and 39. Therefore, claims 34-37 are rejected as being unpatentable over Hellman in view of Schneier and Crandall 5,159,632 for the same reasons set forth in the rejections of claims 32, 33, 38 and 39.

24. As per claims 6-11, they are method claims corresponding to claims 32-37, and they do not teach or define above the information claimed in claims 32-37. Therefore, claims 6-11 are rejected as being unpatentable over Hellman in view of Schneier and Crandall 5,159,632 for the same reasons set forth in the rejections of claims 32-37.

25. As per claims 19-24, they are system claims corresponding to claims 32-37, and they do not teach or define above the information claimed in claims 32-37. Therefore, claims 19-24 are rejected as being unpatentable over Hellman in view of Schneier and Crandall 5,159,632 for the same reasons set forth in the rejections of claims 32-37.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Chang et al. U.S. Patent No. 5,835,592.

Chang U.S. Patent No. 5,987,130.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
August 11, 2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100